Cybersecuritybeleid

Vereniging voor Christelijk Voortgezet Onderwijs te Rotterdam en omgeving

Herkomst document

AUTEUR	ORGANISATIE(ONDERDEEL)
Derk Wieringa, Branko van Ormondt, Ishana Ramsaran en Michiel van Tol	Grant Thornton Specialist Advisory B.V. Cyber Risk Services

Wijzigingshistorie

VERSIE	DATUM	TOELICHTING/WIJZIGINGEN
0.1	23-10-2023	Eerste versie door Grant Thornton
0.2	09-01-2024	Aanpassingen CVO/ T. Mout
0.31	04-04-2024	Aanpassingen door Grant Thornton
0.9	24-04-2024	Versie ter goedkeuring (door Grant Thornton)
1.0	30-05-2024	Versie ter goedkeuring (door Grant Thornton)
1.1	25-11-2024	Aanpassingen na review externe partij

Goedkeuring

ORGANISATIE (ONDERDEEL)	NAAM	FUNCTIE	DATUM	HANDTEKENING
CVO	A. Bestebreur	Lid raad van bestuur	26-11-24	

Verzendlijst

ORGANISATIE (ONDERDEEL)	NAAM	FUNCTIE

Inhoudsopgave

1. Inleiding

Technologie en ICT zijn niet meer weg te denken uit onze samenleving, alles en iedereen is tegenwoordig verbonden. De ontwikkelingen gaan razendsnel en bieden ons volop nieuwe kansen. Helaas spelen kwaadwillende personen actief in op kwetsbaarheden in de technologie en applicaties en zij zorgen ervoor dat onze samenleving dagelijks met de gevolgen van cyberrisico's wordt geconfronteerd. Niet alleen grote commerciële organisaties en de (Rijks)overheid krijgen te maken met cybersecurity-aanvallen, ransomware-aanvallen[1], hacking van systemen en/of datalekken. Ook kleinere bedrijven, gemeenten en onderwijsinstellingen (zoals Scholenkoepel OSG Hengelo en Universiteit Maastricht) zijn inmiddels slachtoffer geweest van het werk van cybercriminelen.

Om CVO hiertegen te beschermen en om als organisatie succesvol te zijn en onze doelstellingen te kunnen realiseren, is cybersecurity voor CVO van cruciaal belang. Door onze cybersecurity goed op orde te hebben, zorgen we ervoor dat we als organisatie weerbaar zijn tegen de risico's in de gedigitaliseerde wereld.

Hierbij hanteren we voor **cybersecurity** de definitie uit het Nederlands Cybersecurity woordenboek:

> *Alle beveiligingsmaatregelen[2] die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.*

Cybersecurity is via deze definitie dus niet beperkt tot ICT. Het is daarom van groot belang dat iedereen binnen CVO weet wat zijn of haar verantwoordelijkheden zijn en wat hij of zij kan doen om de organisatie en onze gegevens veilig te houden.

[1] zie ook het document "Cyberdreigingsbeeld 2021-2022 Onderwijs en Onderzoek" van Surf

[2] Beveiligingsmaatregelen zijn onder te verdelen in maatregelen ten aanzien de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens.

2. Onze visie op cyberweerbaarheid

CVO streeft ernaar dat alle leerlingen die zich bij een CVO-school aanmelden de beste kansen krijgen op succes op school en op een perspectiefrijke toekomst. CVO heeft dan ook een breed onderwijsaanbod, streeft ernaar op alle terreinen kwalitatief goed onderwijs te leveren en heeft aandacht voor de persoonlijke ontwikkeling van iedere leerling.

De ICT-faciliteiten van CVO spelen een zeer belangrijke rol in het onderwijs aan onze leerlingen. Onze verwachting is dat dit in de toekomst nog verder zal toenemen. Onze afhankelijkheid van digitale systemen is daarmee groot en zal naar verwachting groter worden. Daarnaast bevatten deze digitale systemen ook in toenemende mate belangrijke en/of vertrouwelijke gegevens.

Hierbij gaan de ontwikkelingen op het gebied van technologie en cybersecuritydreigingen razendsnel. Om onze visie te kunnen realiseren, kunnen we hierdoor niet meer volstaan met uitsluitend preventieve cybersecuritymaatregelen. De snelle veranderingen vereisen dat wij de effectiviteit van onze cybersecuritymaatregelen continu moeten bewaken en dat we het pakket aan cybersecuritymaatregelen eventueel moeten bijstellen om te kunnen inspelen op actuele ontwikkelingen en nieuwe bedreigingen en kwetsbaarheden.

2.1 Principes cyberweerbaarheid

We willen te allen tijde onze medewerkers en leerlingen een veilige omgeving voor hun data bieden en de continuïteit van onderwijs garanderen. In onze visie ten aanzien van cybersecuritymaatregelen hanteren we daarom de volgende principes:

- **Voorkomen is beter dan genezen**
  We gebruiken preventieve cybersecuritymaatregelen om het kwaadwillende personen zo moeilijk mogelijk te maken. Maar helemaal voorkomen van cybersecurity-incidenten is niet mogelijk. Door kwaadwillende telkens een stap voor te blijven, maken we het cyberrisico zo klein mogelijk.

- **Voorbereiden op een cybersecurity-incident**
  Iedere organisatie krijgt vroeg of laat te maken met een cybersecurity-incident of datalek. Als het ons overkomt, dan moeten we hier goed op voorbereid zijn. Met behulp van een actueel cybercrisisplan kunnen we de impact van een cybersecurity-incident zo beperkt mogelijk houden.

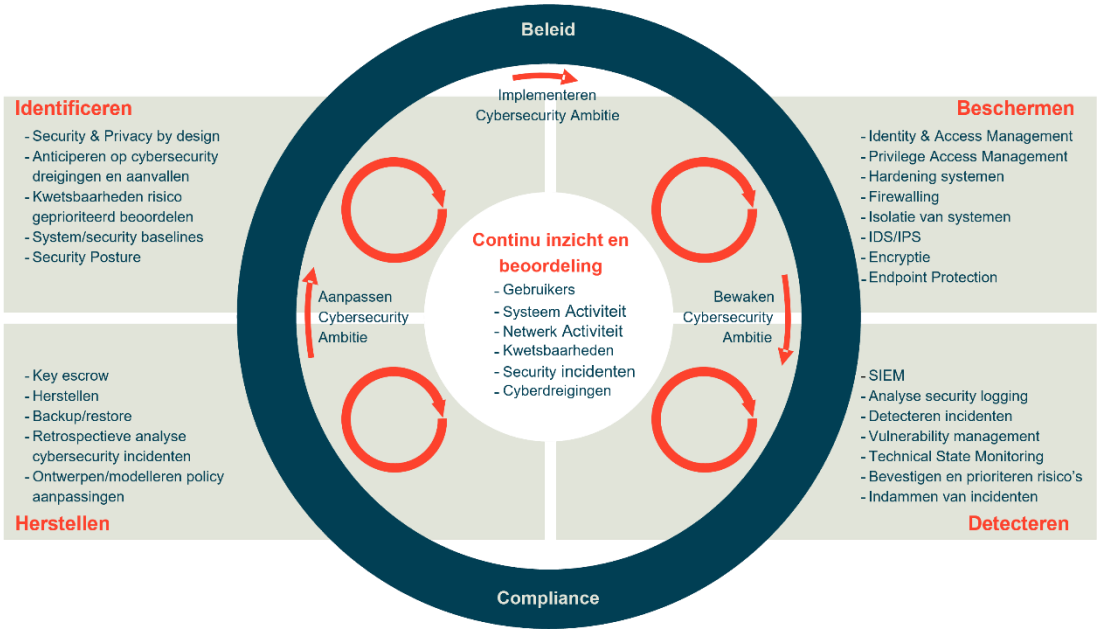
- **Inzicht is cruciaal**
  Inzicht in de werking van onze applicaties, activiteiten van gebruikers en in het voorkomen van kwetsbaarheden in onze omgeving, is van wezenlijk belang. Door onze kwetsbaarheden periodiek in kaart te brengen, relevante gebeurtenissen vast te leggen en te analyseren is het mogelijk om cybersecurity-incidenten vroegtijdig te signaleren of zelfs te voorkomen. Maar ook wanneer een incident is opgetreden, zijn adequate logging en analyse van cruciaal belang. Niet alleen om het incident en de bijbehorende oorzaak te verhelpen, maar ook om onze maatregelen aan te passen zodat we in de toekomst vergelijkbare incidenten kunnen voorkomen.

- **Balanceren tussen bescherming en nut**
  Bij het treffen van cybersecuritymaatregelen besteden we voldoende aandacht aan het aspect van gebruikersgemak. Dit om te voorkomen dat mensen zelf onveilige alternatieven gaan inzetten om hun doel te kunnen bereiken.

- **Cyberweerbaarheid vereist continuïteit**
  Doordat cyberdreigingen zich continu ontwikkelen, betekent stilstand qua ontwikkeling dat we steeds kwetsbaarder worden voor een cybersecurity-incident. Het is daarom van groot belang dat wij onze cyberweerbaarheid continu blijven verbeteren en op een voor CVO adequaat beveiligingsniveau handhaven.

2.2 Model cyberweerbaarheid

Deze principes komen ook tot uitdrukking in onderstaande figuur. Dit figuur is gebaseerd op het Adaptive Security Architecture Framework van Gartner, waarbij gebruik wordt gemaakt van belangrijke elementen uit het NIST Cyber Security Framework.



Deze werkwijze omvat ook een Plan-Do-Check-Act (PDCA)-cyclus waarmee we minimaal jaarlijks op bestuursniveau onze ambitie op het gebied van cybersecurity zullen vaststellen. Om goed weerbaar te zijn tegen cyberrisico's is een samenspel van cybersecuritymaatregelen op het gebied van technologie, processen en mensen nodig. Hierbij onderkennen we de volgende aandachtsgebieden:

- **Continu inzicht hebben**
  De effectiviteit van de cybersecuritymaatregelen moeten we meten en bewaken door continu inzicht te hebben in de activiteiten van het netwerk, de gebruikers en de systemen. Daarnaast is adequaat inzicht in onze kwetsbaarheden en cybersecurity-incidenten nodig. Aan de hand van die inzichten kunnen aanpassingen in onze cybersecuritymaatregelen worden bepaald en geïmplementeerd.

- **Identificeren**
  Het gaat hier enerzijds om het identificeren van onze (digitale) kroonjuwelen. Dit heeft enerzijds betrekking op de gegevens die van grote waarde zijn voor de organisatie op onze medewerkers, leerlingen en de (digitale) systemen waarin onze gegevens zich bevinden. Anderzijds is het van belang om de cyberdreigingen voor onze organisatie en de ontwikkelingen daarin te identificeren. Uitgaande van onze kroonjuwelen en de relevante cyberdreigingen herijken we periodiek onze cybersecurity-ambitie.

- **Beschermen**
  Hierbij gaat het om de preventieve cybersecuritymaatregelen die we treffen om het optreden van cybersecurity-incidenten te voorkomen. Het gaat hierbij om maatregelen waarmee we de kroonjuwelen van CVO beschermen.

- **Detecteren**
  Het gaat hier om het detecteren van kwetsbaarheden en cybersecurity-incidenten. Het loggen van onze relevante cybersecuritygebeurtenissen, analyse en monitoring van deze gebeurtenissen spelen hierin een belangrijke rol. Hierbij zijn goede detectiemiddelen nodig om continu vast te stellen of onze beschermingsmaatregelen goed werken. We moeten kunnen vaststellen of vooraf bedachte risico scenario's

optreden. Daarnaast willen we ook inzicht hebben in afwijkend gedrag in netwerk, systeem, applicatie en van gebruikers.

- **Herstellen**
  We beschikken over plannen en scenario's hoe te handelen als we te maken hebben met een cybersecurity-incident. Naast het acute herstel van het cybersecurity-incident zelf, besteden we hierbij ook aandacht aan de rootcause analyses, zodat we kunnen bepalen of structurele verbetering van ons pallet aan cybersecuritymaatregelen nodig is.

2.3 Ontwerpcriteria cybersecurity

Naast de principes van cyberweerbaarheid uit paragraaf 2.1 en de architectuurprincipes in Architectuurdocument CVO Rotterdam, hanteert CVO de cybersecurity-ontwerpcriteria die hierna worden beschreven. De gedetailleerde invulling van deze ontwerpcriteria wordt uitgewerkt in de onderliggende richtlijnen per onderwerp.

- **Security by design**
  Security by design houdt in dat vanaf het ontwerp van een nieuw systeem of product rekening wordt gehouden met cybersecurity-eisen. Hierdoor worden beveiligingslekken proactief geminimaliseerd in plaats van achteraf te reageren op ontstane cyberdreigingen. Daarnaast is het goedkoper en effectiever om cybersecurity-maatregelen vanaf het begin mee te nemen in de realisatie dan om cybersecuritymaatregelen achteraf toe te voegen. CVO zorgt ervoor dat producten en systemen ingebouwde passende cybersecuritymaatregelen bevatten.

- **Privacy by design**
  Privacy by design houdt in dat vanaf het ontwerp van een nieuw systeem of product rekening wordt gehouden met privacy-eisen. Hierdoor wordt een zorgvuldige omgang met persoonsgegevens afgedwongen in een vroeg stadium en worden inbreuken op privacy proactief voorkomen. CVO zorgt ervoor dat de standaardinstellingen van producten of systemen zo privacy-vriendelijk mogelijk zijn.

- **Zero trust**
  Zero trust betekent dat gebruikers, systemen en netwerken niet zonder meer (automatisch) worden vertrouwd. Gebruikers en hun ICT-faciliteiten moeten worden geïdentificeerd en geauthentiseerd, voordat een gebruiker toegang krijgt tot gegevens van CVO.
  CVO maakt gebruik van conditional access control om het zero trust principe te implementeren. Door middel van conditional access control wordt bij de toegangscontrole gebruik gemaakt van contextuele informatie om het verlenen van toegang te bepalen. Toegang tot data kan uitsluitend worden verkregen door de juiste persoon, op de juiste plek, op het juiste moment, via een beveiligde verbinding. Dit betekent dat een device of persoon uniek identificeerbaar moet zijn om toegang te krijgen tot diensten, applicaties en/of data. Daarmee is het delen van accounts dus niet toegestaan.

- **Identity & Access Management (IAM)**
  Het beheren van identiteiten en de toegang die wordt uitgegeven, worden samen beheerd in een sluitend IAM-proces. De instroom, doorstroom en uitstroom van identiteiten en accounts sluit naadloos aan op de HR-processen rondom in-, door- en uitstroom van personeel en de leerlingenadministratie in Somtoday. Ieder account in een systeem van CVO is te herleiden naar een natuurlijk persoon met een actieve status in de personeels- of leerlingenadministratie. De toegang die aan het account is toegekend, komt overeen met de toegang die nodig is om de functie uit te voeren. Periodiek worden controles uitgevoerd om vast te stellen dat alle actieve accounts en alle toegekende toegangsrechten nog correct zijn.

- **Least access**
  Het least access principe betekent dat iedere gebruiker alleen toegang krijgt tot ICT-faciliteiten en organisatiegegevens die nodig zijn om zijn/haar taken uit te voeren. Hierdoor wordt het kwaadwillenden bemoeilijkt om ongeautoriseerde toegang tot ICT-faciliteiten en organisatiegegevens van CVO te verkrijgen.

Een persoon krijgt alleen de rechten die minimaal nodig zijn op basis van de rol die deze persoon vervult binnen de CVO-organisatie. Deze rollen met bijbehorende rechten worden in het kader van IAM-beleid vooraf vastgesteld en geïmplementeerd.

- **Least privilege**
  Het least privilege-principe betekent dat iedere gebruiker alleen de rechten en bevoegdheden krijgt tot ICT-faciliteiten en organisatiegegevens die nodig zijn om zijn/haar taken uit te voeren. Hierdoor wordt het kwaadwillenden bemoeilijkt om toegang te krijgen tot kritieke ICT-faciliteiten en gevoelige gegevens van CVO via een gebruikersaccount met lage rechten.

- **Functiescheiding**
  Door middel van functiescheiding worden conflicterende taken en verantwoordelijkheden van elkaar gescheiden. Hierdoor verlaagt CVO de kans op onbevoegde of onbedoelde wijzigingen of misbruik van organisatiemiddelen.

- **Defence in depth**
  Met het defence in depth-principe worden diverse beveiligingsmechanismen en -controles in lagen aangebracht om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en systemen te waarborgen. Dit betekent controle op wie toegang heeft tot het netwerk, waarbij de vast te stellen bronsystemen leidend zijn en een eigenaar hebben. Daar start de verantwoordelijkheid wie toegang heeft tot diensten, applicaties en data. Geautomatiseerd worden accounts aangemaakt en ook weer opgeruimd om de integriteit te waarborgen. CVO treft op meerdere plekken cybersecuritymaatregelen en zorgt ervoor dat deze elkaar versterken en aanvullen. Als een cyberdreiging een maatregel ondermijnt, dan heeft de organisatie aanvullende maatregelen getroffen die deze dreiging kunnen tegenhouden zich verder binnen organisatie te verspreiden.

3. Cybersecurity binnen CVO

Bij cybersecurity wordt veelal gedacht aan technische ICT-oplossingen om een organisatie weerbaar te maken tegen kwaadwillende cyberaanvallen, maar dit is slechts een gedeelte van de maatregelen die we treffen. Cybersecurity gaat vooral ook om mensen en processen. Goede cybersecurity vereist in de kern dat iedereen binnen de organisatie weet hoe hij of zij daaraan kan bijdragen.

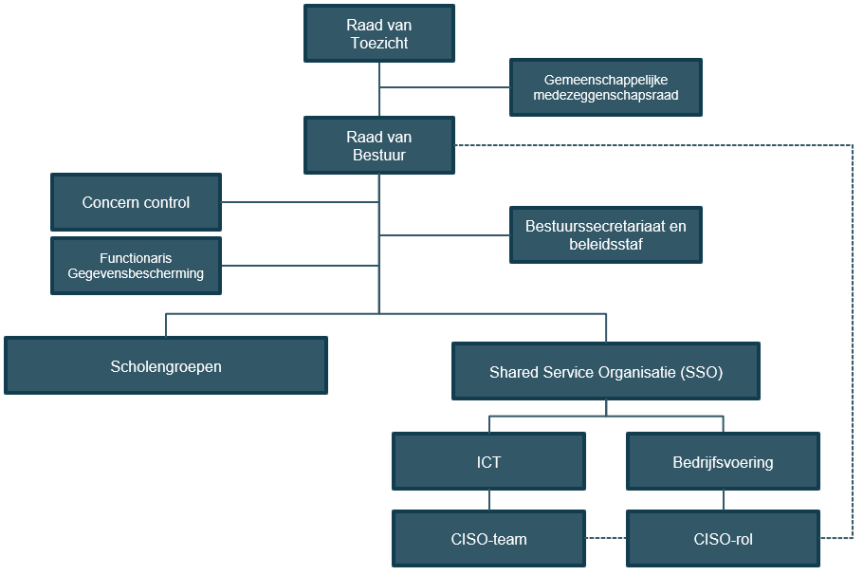
De eindverantwoordelijkheid voor het niveau van cyberweerbaarheid van CVO ligt bij de raad van bestuur van CVO. Binnen CVO onderkennen we de CISO-rol (Chief Information Security Officer). Deze rol ondersteunt de organisatie als expert op het gebied van cybersecurity.

Het vervolg van dit hoofdstuk gaat dieper in op het werkveld en de aandachtsgebieden van de CISO-rol binnen CVO. Hoofdstuk 4 gaat dieper in op de taken en verantwoordelijkheden van zowel de CISO-rol als de andere onderdelen van de organisatie die een rol spelen bij het realiseren van een passend niveau van cyberweerbaarheid. De CISO-rol zoals in dit document wordt beschreven, is nog niet toegewezen. Om deze rol invulling te geven en de organisatie hierop in te richten, is een Kwartiermaker aangesteld. Deze (tijdelijke) projectorganisatie wordt beschreven in hoofdstuk 5.

3.1 CISO-rol

De CISO (Chief Information Security Officer) heeft een unieke positie binnen CVO. De CISO-rol is de verbindende factor tussen de organisatieonderdelen en de ICT-afdeling op het gebied van cybersecurity. De CISO-rol denkt vanuit beide perspectieven om tot een werkbaar en optimaal niveau van cyberweerbaarheid te komen. Hierbij geeft de CISO-rol aan hoe de cybersecurity zal moeten worden vormgegeven en hoe dit in de organisatie zal worden geïmplementeerd.

De CISO-rol ontwikkelt de strategie en het beleid van CVO gericht op cyberweerbaarheid. Tevens ziet de CISO-rol toe op de realisatie van dit beleid. De CISO-rol geeft ook richting aan de cybersecuritymaatregelen die CVO implementeert. De afdeling ICT is verantwoordelijk voor het implementeren, uitvoeren en onderhouden van de nodige cybersecuritymaatregelen. Onderstaand organogram geeft de positie van de CISO-rol binnen de CVO-organisatie weer. De CISO-rol rapporteert aan de directeur bedrijfsvoering en heeft een directe functionele rapportagelijn naar de raad van bestuur.



2.3 CISO-team

Binnen CVO is ervoor gekozen om de strategische, tactische en operationele cybersecurity-expertises te concentreren in één team binnen de organisatie. Het CISO-team is samengesteld uit diverse rollen. De basis van het CISO-team bestaat uit de IT Security Officers. Daarnaast wisselt de samenstelling voor de uitvoering van verschillende taken en verantwoordelijkheden. Bijvoorbeeld in het geval de cybersecuritymaatregelen van een applicatie worden geanalyseerd, wordt de applicatiebeheerder voor dat onderdeel in het CISO-team opgenomen. De meeste leden van het CISO-team vallen hiërarchisch binnen de ICT-afdeling, maar worden voor de CISO-team taken en verantwoordelijkheden operationeel geleid door de CISO-rol.

3.3 Werkveld

De CISO-rol denkt mee en heeft taken op verschillende niveaus binnen CVO. Zo voert de CISO-rol op strategisch niveau taken uit door beleid en richtlijnen op te stellen en de raad van bestuur te adviseren over de koers van CVO op het gebied van cybersecurity en cyberweerbaarheid.

Op tactisch niveau denkt de CISO-rol mee over bijvoorbeeld de informatiearchitectuur. Daarnaast is de CISO-rol ook betrokken bij de interne controle binnen cybersecurity gerelateerde processen.

Operationele taken kunnen voor de CISO-rol bestaan uit het direct adviseren van en/of overleggen met de product owners en applicatiebeheerders en de bijbehorende leveranciers over hoe de cybersecurity bij de betreffende applicaties en systemen horen te zijn ingericht. Het CISO-team voert, desgewenst samen met de externe partner, cybersecuritytests en cybersecuritymonitoring uit. Ook ontwikkelt en onderhoudt het CISO-team een cybersecuritydashboard en -metrics, gebaseerd op het Normenkader IPB FO. Op basis van het cybersecuritydashboard wordt door de CISO-rol gerapporteerd naar onder andere de manager ICT, de directie van de SSO en de raad van bestuur.

3.4 Mensen en processen

Mensen zijn cruciaal wanneer het aankomt op het niveau van cyberweerbaarheid. De mooiste technische oplossingen zijn slechts beperkt effectief als de gebruikers niet weten hoe ze hiermee moeten omgaan.

Het CISO-team analyseert periodiek de huidige processen op cybersecurity-aspecten en zal beoordelen waar deze verbetering behoeven. Met de aanbevelingen van het CISO-team voor deze processen, kunnen we ervoor zorgen dat het niveau van cyberweerbaarheid op het vereiste dan wel het gewenste niveau komt en blijft.

Een ander belangrijk aspect is de cybersecurity-awareness van de medewerkers en leerlingen van CVO. Aanvallers (cybercriminelen of hackers) kiezen om hun doel te bereiken vaak voor een route via een zwakke schakel. Een gebruiker die zich onvoldoende bewust is van de cybersecurityrisico's kan zo'n zwakke schakel zijn. Het is daarom belangrijk om alle medewerkers en leerlingen bewust te maken van de risico's en ze te helpen om hun eigen verantwoordelijkheid hierin te nemen.

3.5 Samenwerking

Eén van de principes die in cybersecurity worden toegepast is die van zogenoemde "defence in depth". Dit principe houdt in dat op meerdere plekken cybersecuritymaatregelen worden getroffen en dat zorgt ervoor dat deze elkaar versterken en aanvullen.

Het is dan ook van belang dat alle medewerkers en afdelingen die te maken hebben met cybersecuritymaatregelen contact hebben met het CISO-team en dit team weten te vinden voor advies en eventuele begeleiding.

Als expert op gebied van cybersecurity van CVO, moet de CISO-rol een oordeel kunnen geven over de juiste werking van alle lagen van cybersecurity. Het is de taak van de CISO-rol om inzicht te hebben in zowel de lopende als nieuwe zaken op het gebied van cybersecurity binnen de verschillende onderdelen en afdelingen van CVO. De CISO-rol heeft hiermee een totaalbeeld van de werking van alle cybersecuritymaatregelen, kan op basis van eigen expertise en

ervaring vaststellen wat zwakke punten zijn en op basis daarvan advies uitbrengen over aanscherping van cybersecuritymaatregelen.

4. Taken en verantwoordelijkheden

Om als organisatie goed weerbaar te zijn en goed in te kunnen spelen op een continu ontwikkelend en veranderend dreigingslandschap, moeten de taken en verantwoordelijkheden op het gebied van cybersecurity helder in de organisatie belegd zijn. In dit hoofdstuk worden de taken en verantwoordelijkheden inzake cybersecurity van de direct betrokkenen gedefinieerd.

De taken en verantwoordelijkheden inzake cybersecurity, zoals beschreven in dit hoofdstuk, geven de ambitie weer waar CVO aan wil voldoen. Delen hiervan zullen daarom in een later stadium, plateau 3 van het programmaplan Cyberweerbaarheid, worden gerealiseerd. Hoofdstuk 5 beschrijft waar de taken en verantwoordelijkheden inzake cybersecurity in huidige fase van ontwikkeling (plateau 1 en 2) afwijken.

4.1 Raad van bestuur

De eindverantwoordelijkheid voor het niveau van cyberweerbaarheid van CVO ligt bij de raad van bestuur. Zij stelt hiertoe de beleidskaders vast en laat zich adviseren door de CISO-rol over het passend niveau van cyberweerbaarheid voor CVO.

Op jaarlijkse basis stelt de raad van bestuur de ambitie op het gebied van cybersecurity vast. Zij wordt hierbij geadviseerd door de CISO-rol.

4.2 CISO-rol

De taken en verantwoordelijkheden van de CISO-rol liggen op de volgende resultaatgebieden:

Beleid

- Vormt zich een visie op de betekenis van cyberweerbaarheid voor CVO, door voortdurende beeldvorming over dreigingen, risico's en oplossingsrichtingen voor maatregelen passend bij het algemene beleid van CVO.
- Stelt doelen voor cyberweerbaarheid voor.
- Ontwikkelt een strategie om die doelen te bereiken.
- Ontwikkelt beleid ter uitvoering van de strategie en stelt het jaarplan cyberweerbaarheid samen.

Leidinggeven

- Geeft sturing aan de organisatorisch kant van cybersecurity.
- Treedt op als opdrachtgever voor CVO-brede projecten op het gebied van cyberweerbaarheid m.b.t. beleid, governance en awareness.
- Organiseert en faciliteert overleg voor sturing en coördinatie op het gebied van cyberweerbaarheid m.b.t. beleid, governance en awareness.

Implementeren

- Bevordert het ontwikkelen van richtlijnen voor cybersecurity en geeft hier richting aan.
- Initieert voorlichtings- en cybersecurity-awareness programma's en geeft hier richting aan.
- Voert de voorlichtings- en cybersecurity-awareness programma's uit en beantwoordt vragen uit de organisatie hierover.
- Initieert en faciliteert risico- en dreigingsanalyses op het gebied van cybersecurity en informatiebeveiliging, bv. risicomanagement d.m.v. de zero trust strategie.
- Toetst cybersecurityrichtlijnen aan het beleid en adviseert zo nodig over verbetering.
- Maakt de opzet voor verbetering van cybersecurityrichtlijnen.
- Bereidt beslissingen op het gebied van cyberweerbaarheid voor.
- Adviseert de raad van bestuur van CVO en diverse organisatieonderdelen (zoals directie SSO, directies van scholen(groepen), afdelingen SSO) bij beleidsbeslissingen met consequenties voor cybersecurity.

Evalueren

- Beoordeelt rapportages van de ICT-afdeling en de leveranciers over de naleving van cybersecurityrichtlijnen en eisen die zijn gesteld.
- Beoordeelt rapportages van in- en externe audits aan de hand van het normenkader IBP FO op relevantie voor cybersecurity.
- Geeft opdrachten tot het verrichten van interne/externe onderzoeken en audits aangaande cybersecurity.
- Beoordeelt periodiek de centrale registratie van cybersecurity-incidenten en de afhandeling daarvan.
- Identificeert, analyseert en evalueert informatiebeveiligingsrisico's (risicobeheer).
- Beoordeelt ontwikkelingen in de maatschappij, de branche en het vakgebied (o.a. ontwikkelingen van dreigingen, aanvalspatronen en cybersecuritymaatregelen).
- Neemt bovenstaande zaken mee in de MARAP en in de PDCA-cyclus.

Onderhouden

- Stelt visie, strategie en beleid inzake cyberweerbaarheid bij en bevordert aanpassing van cybersecurityrichtlijnen op basis van evaluaties.

Contacten en stakeholders

- Onderhoudt contacten met diverse interne stakeholders, in alle lagen van de organisatie. Dit varieert van het adviseren van de raad van bestuur en vertegenwoordiging vanuit directieoverleg (DO), bedrijfsvoerdersoverleg (BO), het afstemmen van communicatie met de afdeling Communicatie/PR tot overleg met medewerkers.
- Onderhoudt externe contacten met bijvoorbeeld auditors, leveranciers, branche- en beroepsgenoten.

Reguliere overleggen (intern)

- 1x per week: Manager ICT
  Regulier overleg tussen de CISO-rol en manager ICT waarin lopende en aankomende wijzigingen en cyberdreigingen worden besproken.
- 1x per maand: Risicomanagement
  Regulier overleg waarin de status van bekende risico's en een analyse van nieuwe risico's worden besproken, onder leiding van de CISO-rol. Hierbij aanwezig zijn de concern controller, manager ICT, CISO-team. Risico's worden gerapporteerd aan de raad van bestuur.
- 1x per maand: directie SSO
- 4x per jaar: raad van bestuur
- 4x per jaar: Privacy officers
- 4x per jaar: ICT-afdeling
- 1x per jaar: manager HR-diensten
- 1x per jaar: manager Financiën
- 1x per jaar: manager Facilitaire diensten

4.3 CISO-team

De taken en verantwoordelijkheden van het CISO-team liggen op de hieronder beschreven resultaatgebieden. Het CISO-team is samengesteld uit verschillende rollen, niet alle rollen zijn hiërarchisch onderdeel van het team. Het CISO-team wordt operationeel aangestuurd door de CISO-rol, maar is hiërarchisch geplaatst in de afdeling ICT.

Beleid

- Ondersteunt de CISO-rol door middel van voorbereidend werk en uitvoering van onderzoek.
- Denkt actief mee ten aanzien van de cyberweerbaarheidsstrategie.
- Ondersteunt de CISO-rol bij het maken van conceptrichtlijnen op het gebied van (technische) cybersecuritymaatregelen.

Implementeren

- Ontwikkelt de (technische) cybersecurityrichtlijnen.

- Voert de voorlichtings- en cybersecurity-awareness programma's uit en beantwoordt vragen uit de organisatie hierover.
- Voert risico- en dreigingsanalyses uit op gebied van cybersecurity en informatiebeveiliging.
- Maakt de opzet voor de verbetering van cybersecurityrichtlijnen.
- Ontwerpt of beheert zelfstandig cybersecuritymaatregelen die onderdeel zijn van de technische infrastructuur.
- Adviseert over de implementatie en het gebruik van cybersecuritymaatregelen in de technische infrastructuur van leveranciers door middel van de richtlijn voor leveranciers.
- Voert cybersecurity monitoring werkzaamheden uit.
- Bereidt de periodieke rapportages en/of dashboards over de actuele status van (technische) cybersecurity voor.

Evalueren

- Voert onderzoek uit naar de ontwikkelingen op het gebied van cybersecuritymaatregelen en cybersecuritydreigingen;
- Voert zelfstandig (live) testen uit om cybersecuritykwetsbaarheden in de organisatie, de applicaties of de technische infrastructuur te kunnen vaststellen. Evt. met externe partner.
- Is betrokken bij het analyseren en afhandelen van cybersecurity-incidenten.

Onderhouden

- Draagt zorg voor het mitigeren van kwetsbaarheden die ontdekt zijn tijdens een cybersecuritytest of -incident.

4.4 ICT-afdeling

De afdeling ICT is voor de CVO-medewerkers het eerste aanspreekpunt bij ICT-gerelateerde zaken en/of problemen. Hierdoor heeft de afdeling ICT goed zicht op zowel alle incidenten als op alle verzoeken tot wijziging die binnen de CVO-organisatie spelen. Het is de verantwoordelijkheid van de afdeling ICT om bij alle incidenten en wijzigingsverzoeken te signaleren of aan het incident of de wijziging ook een cybersecurity en/of privacy aspect zit. Daar waar nodig moet tijdig afstemming met de CISO-rol en manager ICT plaatsvinden.

4.5 Afdelingsmanager/proceseigenaar

Een afdelingsmanager/proceseigenaar heeft binnen CVO de bevoegdheid om te bepalen hoe een proces verloopt, en heeft de verantwoordelijkheid ervoor te zorgen dat het proces aan de gebruikersverwachtingen en organisatiedoelstellingen blijft voldoen, vandaag en in de toekomst. De verantwoordelijkheden en taken die hierbij horen zijn:

- Actieve rol in het wijzigingsbeheerproces.
- Accordering van de autorisatiematrix.
- (Mede)beoordelen van geïmplementeerde autorisaties.
- Training van medewerkers voor het proces en applicatiesysteem.
- Contactpersoon voor ICT-afdeling en applicatie-leverancier
- Contactpersoon voor cybersecurity- en privacy-aangelegenheden

4.6 Scholendirecties

Het beleid voor cyberweerbaarheid wordt bij CVO centraal opgesteld en tot uitvoer gebracht zoals beschreven in dit document. Binnen de scholen(groepen) zijn algemene directies en vestigingsdirecteuren mede verantwoordelijk voor het correct uitvoeren van dit beleid. De verantwoordelijkheden en taken die hierbij horen zijn:

- Bepalen van de impact op de scholengroep en beleggen van acties die binnen de scholengroep uitgevoerd moeten worden.
- (Mede)beoordelen van geïmplementeerde autorisaties.
- Contactpersoon voor ICT-servicemanager CVO.
- Contactpersoon voor cybersecurity-aangelegenheden.

4.7 Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) ontfermt zich binnen CVO over de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG heeft de volgende taken en verantwoordelijkheden:

- Informeren en adviseren van CVO-medewerkers over gegevensbescherming.
- Contact onderhouden met coördinator IBP.
- Toezicht houden op naleving van de AVG.
- Adviseren over de uitvoering van een Data Protection Impact Assessment (DPIA), die de privacyrisico's van gegevensverwerking in kaart brengt.
- Samenwerken met de Autoriteit Persoonsgegevens (AP) en het melden van datalekken.
- Contactpersoon van de Autoriteit Persoonsgegevens (AP).
- Ad-hoc overleggen met de CISO-rol indien een cybersecurity-incident gepaard gaat met een datalek.

4.8 Afdeling HR & Juridische Zaken

De afdeling HR & Juridische Zaken van CVO speelt op het gebied van cybersecurity een belangrijke rol bij de in- en uitdiensttreding van medewerkers en contracteren van externen. De verantwoordelijkheden van deze afdeling zijn:

- Het uitvoeren van een passende "background check" door middel van een VOG-aanvraag.
- Tijdig invoeren van nieuwe medewerkers in het HRM-systeem. Hierbij wordt tevens zorggedragen voor de toekenning van de juiste rol in de organisatie (IAM).
- Tijdig invoeren van wijzingen in het HRM-systeem als gevolg van mutaties bij CVO intern.
- Tijdig invoeren van uitdienst-meldingen in het HRM-systeem.
- Afstemming met de CISO-rol over afwijkingen, wijzigingen en incidenten.

4.9 Facilitaire diensten

Fysieke beveiliging is een belangrijk onderdeel van het totaalpakket aan cybersecuritymaatregelen van CVO. Bij CVO is de afdeling Huisvesting, Facilitair, Inkoop & Contractbeheer verantwoordelijk voor het treffen van passende fysieke beveiligingsmaatregelen in en om de locaties waar zich waardevolle gegevens en/of kroonjuwelen van CVO bevinden. Het betreft onder andere:

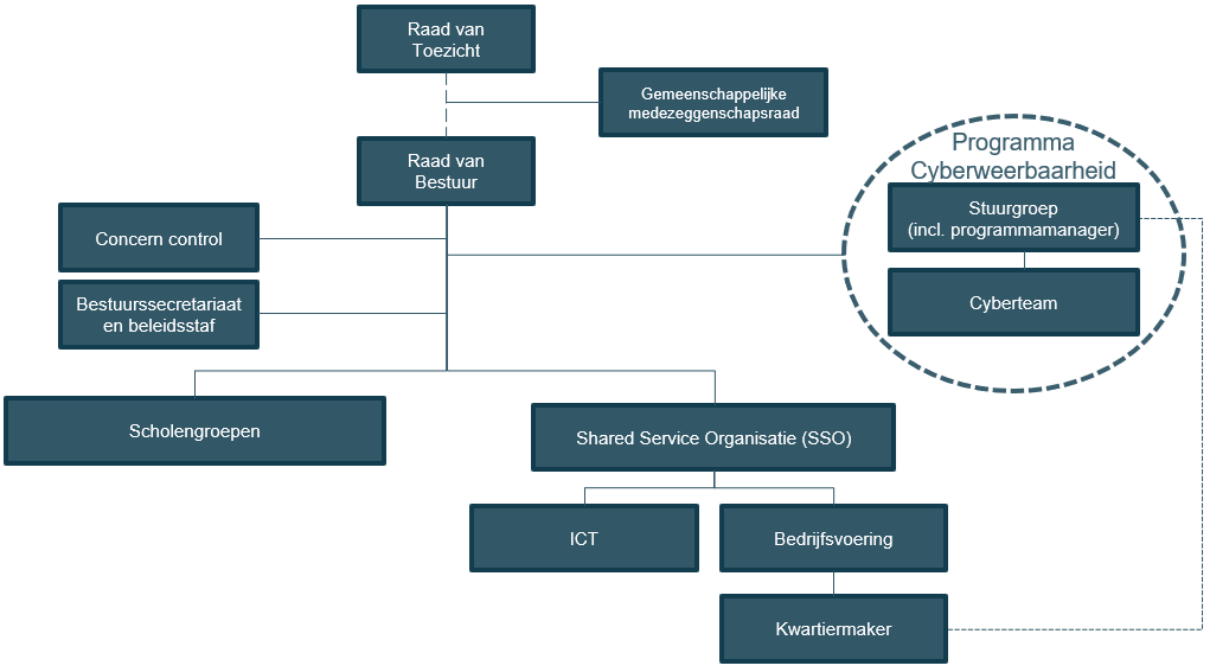
- Adequate fysieke beveiliging (inbraakdetectie, camerabewaking, ruimteconditionering, beperking toegang tot "kroonjuwelen" zoals een kluis, serverruimte (MER/SER), opslagruimte van eventueel gevoelige gegevens) van de CVO-locaties.
- Adequaat beheer van sleutels en toegangspasjes wordt uitgevoerd door lokale facilitaire teams.
- Afstemming met en advisering van lokale facilitaire teams en directies van de scholen(groepen) over te nemen maatregelen op gebied van fysieke beveiliging.
- Afstemming met de CISO-rol over afwijkingen, wijzigingen en incidenten.

4.10 Medewerkers en leerlingen

Iedereen binnen CVO, zowel medewerkers als leerlingen, heeft een rol binnen de cybersecurity van CVO. Iedereen draagt bij aan een veilige(re) omgeving door maatregelen en richtlijnen op te volgen zoals die door de CISO-rol en het CISO-team zijn opgesteld en door de raad van bestuur zijn vastgesteld. Vanuit het CISO-team worden de medewerkers en leerlingen periodiek geïnformeerd over het belang van onze maatregelen. Tevens zal het CISO-team de awareness van de medewerkers en leerlingen blijven ontwikkelen. Het is de verantwoordelijkheid van alle medewerkers en leerlingen van CVO om in geval van een verdachte cybersituatie contact op te nemen met het CISO-team.

5. Programmamanagement en kwartiermaker

De CISO-rol en het CISO-team, zoals beschreven in de voorgaande hoofdstukken, worden ingericht als onderdeel van het programma cyberweerbaarheid (plateau 3). Tot het moment dat de CISO-rol daadwerkelijk is toegewezen, is ervoor gekozen om de strategische, tactische en operationele cybersecurity-expertises te verdelen over twee rollen in de organisatie. Om deze organisatie invulling te geven en neer te zetten, is een kwartiermaker aangesteld. Deze is verantwoordelijk voor het strategisch en tactische deel binnen de organisatie en het opzetten en uitvoeren van een groot deel van de taken van het CISO-team. Het operationele en technische deel wordt geleid door de manager ICT. De kwartiermaker zelf maakt geen onderdeel uit van de ICT-afdeling, maar heeft wel regelmatig overleg met de manager ICT en de ICT-afdeling over de strategische en tactische keuzes. Het aangepaste organogram hieronder geeft voor de duur van het CVO-programma cyberweerbaarheid de tijdelijke CISO-organisatie van CVO weer



5.1 Kwartiermaker

Om de CISO-organisatie invulling te geven en neer te zetten zoals beschreven in dit document, is een kwartiermaker aangesteld. De taken en verantwoordelijkheden van de kwartiermaker betreffen voornamelijk het organisatorische deel van de CISO-rol en het CISO-team. De kwartiermaker rapporteert aan de directeur bedrijfsvoering van de SSO en heeft een functionele rapportagelijn naar de stuurgroep van het programma cyberweerbaarheid.

Beleid

- Vormt zich een visie op de betekenis van cyberweerbaarheid voor CVO, door voortdurende beeldvorming over dreigingen, risico's en oplossingsrichtingen voor maatregelen passend bij het algemene beleid van CVO.
- Stelt doelen voor cyberweerbaarheid voor.
- Ontwikkelt een strategie om die doelen te bereiken.
- Ontwikkelt beleid ter uitvoering van de strategie en stelt het jaarplan cyberweerbaarheid samen.
- Ontwikkelt risicobeheerplan.
- Ontwikkelt en onderhoudt het Incident Respons Plan.
- Ontwikkelt en onderhoudt beleidsrichtlijnen en procedures, waaronder: toegangscontrole, gegevensbescherming. incident respons, naleving/ verankering in de staande organisatie up-to-date.
- Ziet toe op naleving relevante wet- en regelgeving.

Leidinggeven

- Geeft sturing aan de organisatorische kant van cybersecurity.
- Treedt op als opdrachtgever voor CVO-brede projecten op het gebied van beleid, governance en awareness met betrekking tot cyberweerbaarheid.
- Organiseert en faciliteert overleg voor sturing en coördinatie op het gebied van beleid, governance en awareness met betrekking tot cyberweerbaarheid.
- Coördineert bij een beveiligingsincident.

Implementeren

- Bevordert het ontwikkelen van cybersecurityrichtlijnen en geeft hier richting aan.
- Initieert voorlichtings- en cybersecurity-awareness programma's en geeft hier richting aan.
- Voert de voorlichtings- en cybersecurity-awareness programma's uit en beantwoordt vragen uit de organisatie hierover.
- Initieert en faciliteert risico- en dreigingsanalyses op gebied van cybersecurity en informatiebeveiliging door middel van de zero trust strategie.
- Toetst cybersecurity-richtlijnen aan het beleid en adviseert zo nodig over verbetering.
- Maakt de opzet voor de verbetering van cybersecurityrichtlijnen.
- Bereidt beslissingen op het gebied van cyberweerbaarheid voor.
- Adviseert de raad van bestuur van CVO, organisatieonderdelen van CVO en de afdeling ICT bij beleidsbeslissingen met consequenties voor cybersecurity.

Evalueren

- Beoordeelt rapportages van de ICT-afdeling en de leveranciers over de naleving van cybersecurity-richtlijnen en eisen die zijn gesteld.
- Beoordeelt rapportages van in- en externe audits op relevantie voor cybersecurity.
- Geeft opdrachten tot het verrichten van in-/externe onderzoek en audits aangaande cybersecurity.
- Beoordeelt periodiek de centrale registratie van cybersecurity-incidenten en de afhandeling daarvan.
- Identificeert, analyseert en evalueert informatiebeveiligingsrisico's (risicobeheer);
- Beoordeelt ontwikkelingen in de maatschappij, de branche en het vakgebied (o.a. ontwikkelingen van dreigingen, aanvalspatronen en cybersecuritymaatregelen).

Onderhouden

- Stelt de visie, strategie en beleid inzake cyberweerbaarheid bij en bevordert aanpassing van cybersecurityrichtlijnen op basis van evaluaties.

Contacten en stakeholders

- De kwartiermaker onderhoudt contacten met diverse interne stakeholders, in alle lagen van de organisatie. Dit varieert van het adviseren van de raad van bestuur en vertegenwoordigers vanuit het directieoverleg (DO), bedrijfsvoerdersoverleg (BO), het rapporteren aan de programmamanager, het afstemmen van communicatie met de afdeling PR/communicatie tot overleg met medewerkers.
- De kwartiermaker onderhoudt externe contacten met bijvoorbeeld auditors, leveranciers, branche- en beroepsgenoten.

Reguliere overleggen (intern)

- 1x per week: Manager ICT
  Regulier overleg tussen de CISO-rol en manager ICT, waarin lopende en aankomende wijzigingen en cyberdreigingen worden besproken.
- 1x per maand: Risicomanagement
  Regulier overleg waarin de status van bekende risico's en een analyse van nieuwe risico's worden besproken, onder leiding van de CISO-rol, aanwezig: concerncontroller, manager ICT, CISO-team. Risico's worden gerapporteerd aan de raad van bestuur.
- 1x per maand: Directie SSO

- 4x per jaar: Raad van bestuur
- 4x per jaar: Privacy officers
- 4x per jaar: ICT-afdeling
- 1x per jaar: Manager Financiën
- 1x per jaar: Manager HR-diensten & Inkoop
- 1x per jaar: Manager Huisvesting, Facilitair, Inkoop & Contractbeheer

5.2 Manager ICT

De CISO-rol is nog niet toegekend, maar de taken en verantwoordelijkheden van deze rol worden op dit moment verdeeld tussen de kwartiermaker en de manager ICT. De manager ICT is, tot de benoeming van een CISO, verantwoordelijk voor de technische kant van de CISO-rol. De manager ICT heeft voor deze taken en verantwoordelijkheden een functionele rapportagelijn naar de stuurgroep van het programma cyberweerbaarheid.

De taken en verantwoordelijkheden van de manager ICT liggen op de volgende resultaatgebieden:

Beleid

- Ondersteunt de kwartiermaker door middel van voorbereidend werk en uitvoering van onderzoeken.
- Denkt actief mee ten aanzien van de cyberweerbaarheidsstrategie.
- Ondersteunt de kwartiermaker bij het maken van concept-beleid en -richtlijnen op het gebied van (technische) cybersecuritymaatregelen.
- Stelt richtlijnen op voor het veilig gebruik van ICT-middelen.
- Stelt architectuurprincipes op en onderhoudt deze.
- Legt ontwerpvoorstellen ter besluitvorming voor aan de stuurgroep.

Implementeren

- Ontwikkelt de (technische) cybersecurityrichtlijnen.
- Voert risico- en dreigingsanalyses op het gebied van cybersecurity en informatiebeveiliging uit.
- Ontwerpt en beheert zelfstandig cybersecuritymaatregelen die onderdeel zijn van de technische infrastructuur.
- Adviseert over de implementatie en het gebruik van cybersecuritymaatregelen in de technische infrastructuur van leveranciers door middel van de richtlijn voor leveranciers.
- Voert cybersecuritymonitoring werkzaamheden uit.
- Bereidt de periodieke rapportages en/of dashboards over de actuele status van (technische) cybersecurity voor.
- Zorgt voor verankering vanuit het programma in de staande organisatie.
- Voert Disaster Recovery testen uit.

Evalueren

- Voert onderzoek uit naar de ontwikkelingen op het gebied van cybersecuritymaatregelen en cybersecuritydreigingen.
- Voert zelfstandig (live) testen uit om cybersecuritykwetsbaarheden in de organisatie, de applicaties of de technische infrastructuur te kunnen vaststellen. Eventueel in samenwerking met een externe partner.
- Is betrokken bij het analyseren en afhandelen van cybersecurity-incidenten.

Onderhouden

- Draagt zorg voor het mitigeren van kwetsbaarheden die ontdekt zijn tijdens een cybersecuritytest en -incident.

5.3 Programmamanager Cyberweerbaarheid

De CISO-rol is nog niet toegekend, maar de taken en verantwoordelijkheden van deze rol worden verdeeld tussen de kwartiermaker en de manager ICT. Beide rollen hebben voor deze taken en verantwoordelijkheden een functionele

rapportagelijn naar de Stuurgroep van het programma cyberweerbaarheid. Het programma cyberweerbaarheid wordt aangestuurd door de programmamanager.

De taken en verantwoordelijkheden van de programmamanager liggen op de volgende resultaatgebieden:

- Rapporteren over de voortgang van het programma aan stuurgroep en directie SSO.
- Bewaken en afstemmen voortgang met de manager ICT en de kwartiermaker.

5.4 Cyberteam

Het cyberteam is onderdeel van het programma Cyberweerbaarheid. Het team is samengesteld om de deelprojecten, zoals beschreven in het programmaplan cyberweerbaarheid, uit te voeren. Voortgangrapportages en documenten ter besluitvorming worden aangeboden aan de stuurgroep van het programma cyberweerbaarheid.

5.5 Stuurgroep programma cyberweerbaarheid

De CISO-rol is nog niet toegekend, maar de taken en verantwoordelijkheden van deze rol worden verdeeld tussen de Kwartiermaker en de manager ICT. Beide rollen hebben voor deze taken en verantwoordelijkheden een functionele rapportagelijn naar de Stuurgroep van het programma cyberweerbaarheid.

De taken en verantwoordelijkheden van de stuurgroep liggen op de volgende resultaatgebieden:

- De stuurgroep is verantwoordelijk voor de realisatie van het programma cyberweerbaarheid, doorvertaling van het programma naar plateau 3 en vertaling vanuit het programma naar de staande organisatie;
- De stuurgroep is verantwoordelijk voor de rapportage naar de raad van bestuur. Daarnaast informeert de stuurgroep het BO en DO, de GMR, leerlingen, ouders en overige gebruikers;
- Vaststellen en realiseren cyberweerbaarheid-beleid CVO breed;
- Bepalen strategische koers van het programma;
- Kennisnemen van cyberrisico’s voor CVO en toezien dat CVO voldoet aan wet- en regelgeving;
- Verantwoordelijk voor naleving cybersecurity-afspraken binnen CVO;
- Creëren van een cultuur van cybersecuritybewustzijn binnen CVO.

6. Toepassingsgebied

Dit beleid is van toepassing op alle onderdelen van de CVO-organisatie:

- Alle scholengroepen en aangesloten scholen;
- Shared Service Organisatie (SSO);
- Raad van bestuur CVO;
- Beleidsstaf (CBS);
- CVO Academie.

7. Werking

Dit cybersecuritybeleid treedt in werking na vaststelling door de raad van bestuur van CVO.

8. Periodieke herziening

Minimaal eens per jaar wordt dit document herzien door de CISO-rol. Indien wijzigingen in dit document plaats dienen te vinden, dient de herziening ter goedkeuring te worden aangeboden aan de raad van bestuur.

9. Bronnen

Bij het opstellen van het CVO-cybersecuritybeleid is gebruik gemaakt van de volgende bronnen:

- Gartner Adaptive Cyber Security Framework
- NIST Cyber Security Framework
- ISO/IEC 27000-serie